PhishCloud Operational Technology Detection Engineering Services

PhishCloud Detection Engineering Services reduce alert noise, close IT-to-OT detection gaps, and turn existing security tools into measurable detection capability across industrial environments.

PHISHCLOUD
Protect The Click. Defend The Core.

SERVICES

- OT-Aware Detection Logic
- IT-to-OT Pivot Detection
- MITRE ATT&CK Enterprise + ICS Coverage
- False-Positive Reduction
- Detection-as-Code Lifecycle Management

The Problem

Many industrial and converged-environment operators own detection tools. Few own detection capability.

SIEMs, EDRs, NDR platforms, and OT monitoring tools generate alerts, but most organizations cannot confidently answer two critical questions: What do we detect? How well does it work? The result is a dangerous gap between security visibility and operational protection.

Organizations commonly struggle with:

- SIEM rules that produce volume without fidelity.
- OT-specific TTPs that go undetected.
- Industrial protocols such as Modbus, DNP3, S7, OPC-UA, and EtherNet/IP passing through the environment without meaningful inspection.
- Purdue Model boundary violations that go unnoticed.
- Detection content that decays as adversary behavior changes.
- Red team, threat hunting, DFIR, and threat intelligence findings that never become durable detection logic.
- Alert fatigue that buries analysts in noise instead of surfacing real threats.

The consequence is predictable. Threats are missed outright or detected only after operational impact.

The Solution: PhishCloud OT Detection Engineering Services

PhishCloud Detection Engineering Services design, develop, tune, validate, and manage detection content across the customer's security stack. This includes:

- SIEM correlation rules.
- EDR behavioral detections.
- NDR analytics.
- OT-specific detection logic.
- IT-to-OT pivot detections.
- Industrial protocol analytics.
- Purdue Model boundary detections.

PhishCloud does not treat detection engineering as a tool deployment. We treat it as an operational discipline. Our service turns your existing platforms into a measurable detection capability that reflects how adversaries actually move across IT, identity, remote access, engineering workstations, and OT environments.

The result is fewer low-value alerts, stronger cross-domain detection coverage, and a detection program that continuously improves through Cyber Fusion Center inputs from threat intelligence, red team findings, threat hunting, and DFIR.

Strategy Components

A structured approach built for converged IT and industrial environments.

- Detection strategy and coverage modeling
- MITRE ATT&CK Enterprise and ICS mapping
- SIEM, EDR, NDR, and OT monitoring content development
- Industrial protocol detection logic
- Purdue-zone-aware detection engineering
- False-positive tuning using operational context
- Detection-as-Code version control and peer review
- Lifecycle management, backlog grooming, and decay tracking
- Detection effectiveness measurement and executive reporting

Why Customers Trust PhishCloud?

Deep OT Detection Expertise. PhishCloud understands that industrial environments are not traditional IT networks. We build detection logic that accounts for industrial protocols, Purdue Model architecture, engineering workflows, maintenance windows, safety requirements, and production realities.

IT-to-OT Pivot Focus. Most detection programs treat OT as a separate monitoring problem. PhishCloud treats the IT-to-OT pivot as a first-class detection target, including identity abuse, jump-host misuse, remote access anomalies, and suspicious movement toward control networks.

Purdue-Zone-Aware Detection Logic. A behavior that is benign at one Purdue level may be critical at another. PhishCloud writes detection content with explicit awareness of where the activity occurs, what boundary it crosses, and what operational risk it creates.

Process-Context False-Positive Suppression. We reduce noise using operational context such as engineering tags, setpoints, batch states, maintenance windows, and known-good process behavior. The goal is not more alerts. The goal is higher-fidelity alerts.

Safety-First Review Gate. Every OT detection is reviewed for process-safety implications before production deployment. PhishCloud does not deploy detection content that could drive unsafe or destabilizing operational decisions.

Detection-as-Code Discipline. Detection content is version-controlled, peer-reviewed, tested, documented, and traceable. Every rule has ownership, logic, ATT&CK mapping, change history, and deployment rationale.

Cyber Fusion Integration. Threat intelligence, red team results, threat hunting findings, and DFIR lessons all feed the detection backlog. Detection Engineering becomes the operational bridge between what PhishCloud learns and what the client can detect next.

OT Detection Engineering Key Deliverables

Typical outputs from the engagement:

Strategy and Coverage

- Detection strategy and coverage model
- Sector-specific threat profile
- MITRE ATT&CK Enterprise and ICS coverage map
- Detection gap analysis across IT, identity, network, and OT environments
- Prioritized detection backlog

Detection Content

- SIEM correlation rules
- Identity-based detections
- IT-to-OT pivot detections
- EDR behavioral detections
- NDR flow-based analytics
- OT monitoring platform detection logic
- Industrial protocol analytics

OT-Specific Engineering

- Modbus, DNP3, S7, OPC-UA, EtherNet/IP, and IEC 60870-5-104 detection logic
- Purdue Model boundary detections
- Unauthorized engineering operation detections
- Anomalous control command detections
- Asset baseline deviation detections

Tuning and Lifecycle

- False-positive management workflow
- Tuning documentation
- Suppression criteria and rationale
- Detection-as-Code repository structure
- Versioning and change control
- Detection retirement and rewrite policy

Metrics and Reporting

- ATT&CK coverage reporting
- Alert fidelity metrics
- Mean Time to Detect measurement
- Detection decay reporting
- Sector TTP coverage reporting
- Quarterly detection effectiveness reviews

OT Detection Engineering Key Benefits

How this helps teams immediately:

- Reduces alert fatigue
- Improves analyst confidence
- Converts existing tools into actual detection capability
- Identifies IT-to-OT attack paths earlier
- Creates defensible detection coverage for auditors, insurers, regulators, and boards
- Improves detection fidelity across industrial environments
- Ensures red team, DFIR, threat hunting, and CTI findings become operationalized

If you own the tools but still cannot prove what you detect, PhishCloud Detection Engineering Services are built for you.

PHISHCLOUD
Protect The Click. Defend The Core.

www.phishcloud.com
sales@phishcloud.com
9 Lake Bellevue Drive
Suite 120
Bellevue, WA 98005